(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 984 630 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.03.2000 Bulletin 2000/10

(51) Int. Cl.[7]: **H04N 7/16**, H04N 7/167

(21) Application number: **98202916.7**

(22) Date of filing: **01.09.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

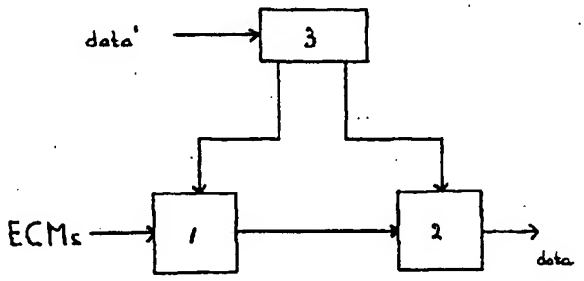
(71) Applicant: **Mindport B.V.**
2130 KA Hoofddorp (NL)

(72) Inventor: **Rix, Simon Paul Ashley**
Germiston, Transvaal (ZA)

(74) Representative:
de Vries, Johannes Hendrik Fokke
De Vries & Metman B.V.,
Overschiestraat 180
1062 XK Amsterdam (NL)

(54) Data communication system

(57) A system for decrypting an encrypted message comprises first and second decryption devices, the first decryption device having a higher security than the second decryption device. The system further comprises means for dividing the encrypted message into blocks, and means for providing at least the first block of the message to the first decryption device and for providing a plurality of further blocks of this message to the second decryption device. An output of the first decryption device is used as input of the second decryption device. The second decryption device operates according to a block chaining method for decrypting the plurality of further blocks.



EP 0 984 630 A1

Description

[0001] The invention generally relates to a data communication system, and more specifically to a system and method for decrypting an encrypted message and a method for broadcasting data.

[0002] Such systems are known in various embodiments and are for example used in a decoder with a conditional access module for pay TV. Generally a secret key is required for decrypting the message, wherein decryption is carried out in a security device in order to prevent unauthorized persons to access the secret key. As security device a smart card can be used, for example. Such a known system using a smart card for decrypting the message shows the disadvantage that the security device has a restricted computing capacity. On the other hand on many locations a computer system with high computing capacity is available, however such systems are easily accessible for unauthorized persons.

[0003] The invention aims to provide a system of the above-mentioned type with a combination of high security and high computing capacity.

[0004] To this end the system for decrypting an encrypted message according to the invention comprises first and second decryption devices, the first decryption device having a higher security than the second decryption device, means for dividing the encrypted message into blocks, and means for providing at least the first block of the message to the first decryption device and for providing a plurality of the further blocks of this message to the second decryption device, wherein an output of the first decryption device is used as input of the second decryption device, said second decryption device operating according to a block chaining method for decrypting said plurality of further blocks.

[0005] In this manner a system is provided wherein the first decryption device having a higher security is used for decrypting a first block of the message only whereafter the remaining part of the message is decrypted by the second decryption device which can have a high computing capacity. The second decryption device can have a low security as the use of a block chaining method makes the insecure decryption device as secure as the first decryption device.

[0006] In order to further enhance security the providing means provides each x^{th} block to the first decryption device according to a further embodiment of the invention. It is noted that the term x^{th} block means that the number of intermediate blocks is not fixed, i.e. may very as desired.

[0007] The invention further provides a method for decrypting an encrypted message, comprising the steps of dividing a message into blocks, decrypting at least the first block in a first decryption device, decrypting a plurality of further blocks in a second decryption device, the first decryption device having a higher security than the second decryption device, using an output of the first decryption device as input of the second decryption device and operating the second decryption device according to a block chaining method.

[0008] The invention will be further explained by reference to the drawing in which an embodiment of the system of the invention is shown in a very schematical manner.

[0009] A system for decrypting a message, for example the encrypted payload in a pay TV transport stream, comprises a first decryption device 1 and a second decryption device 2. The first decryption device has a very high security and is made for example as a smart card. In the smart card a secret key is stored for decryption purposes. The second decryption device 2 has a low security and can be a PC or a microprocessor in a conditional access module or the like.

[0010] The system further comprises means 3 for dividing a message received into blocks, wherein the means 3 provides at least the first block to the first decryption device 1 and a plurality of the further blocks of the message to the second decryption device 2. The first block is decrypted by the device 1 according to the decryption algorithm used and the clear text output is forwarded to the second decryption device 2. The second decryption device 2 decrypts the further blocks according to an error-propagating block chaining method using the clear text output of the device 1 as initialisation vector. In this manner the insecure device 2 is made as secure as the first device 1.

[0011] If desired the means 3 can be arranged in such a manner that each x^{th} block is decrypted by the first decryption device 1.

[0012] It is noted that instead of an error-propagating block chaining method another block chaining method can be used, although an error-propagating method is preferred. Further, the first device could provide a partially decrypted result as output to the second device. In that case the second device would first complete the decryption operation and would then operate according to the block chaining method used.

[0013] The system described can advantageously be used in a pay TV system, wherein entitlement control messages ECMs are used to distribute keys to subscribers, which keys are used to scramble the data. Of course, these ECMs are also encrypted, preferably by using another key, for example a group key. According to a prefered embodiment the data to be distributed is divided into blocks as described, wherein the first block and if desired each x^{th} block of data is scrambled using a first key CW1 and wherein the further blocks are scrambled using a second key CW2 in a block chaining method using the first block and if applicable each x^{th} block as input vector. Both keys CW1 and CW2 are distributed by means of the ECMs.

[0014] At the subscribers the ECMs are provided to the first decryption device or smart card 1 in a usual manner. The smart card 1 decrypts the ECMs and uses the key CW1 to descramble the first block of data (and

each x^{th} block) received from the means 3. The second key CW2 and the first and x^{th} blocks are delivered to the second security device 2, in this case a control access module for example, to descramble the further blocks of data according to the block chaining method used in the system. In this manner it is prevented that the key CW1 which generally contains of 64 bits only, is accessible to unauthorized persons for distribution to other unauthorized persons for descrambling the payload data.

[0015] The system and method described are particularly suitable to prevent a form of piracy which is known in the pay TV industry as "hook" piracy. In this type of piracy the key or control word CW which is used to encrypt the data and which has been determined by a pirate, is rebroadcast by the pirate to receivers which already receive the scrambled data. These receivers then use the key to descramble the data, thereby circumventing the conditional access system of the broadcasting organisation. In pay TV environment this form of piracy has never gained wide usage due to the logistical problems of setting up a broadcast network to rebroadcast the key.

[0016] However, with increasing usage of the internet also for multicasting of broadcasting data, the terminals receiving the scrambled data from the internet can receive data from virtually any other source on the internet simultaneously. Therefore, it is possible to receive the keys required to decrypt the data from an other source, thereby circumventing the conditional access system. Rebroadcasting the key only requires a few bits per second bandwidth thereby making the conditional access system of the data broadcasters vulnerable.

[0017] Although a possible solution to this problem would be to perform the descrambling of the data entirely within the smart card or any other secure device, the ability of a smart card to handle data at high data rates is limited. The current standard bit rate for communicating with a smart card is 9600 bit/s. The real payload throughput is in fact much lower due to overheads on the serial link between the smart card and the conditional access module or the like.

[0018] According to the invention the data to be broadcasted is first divided into blocks and then at least the first data block is encrypted using a first secret key and thereafter a plurality of the further data blocks is encrypted according to an error-propagating block chaining method using the first data block as input vector in a high speed scrambler unit. The scrambled data obtained in this manner is broadcasted and can be descrambled or decrypted in the above described manner. Although the pirate could rebroadcast the output of the smart card, i.e. the descrambled first data block the bandwidth required for rebroadcasting by the pirate is effectivily increased to the maximum rate which is possible on the interface between smart card and conditional access module or the like. As stated above, the amount of data required for rebroadcasting is thereby increased to several kilobits per second as opposed to the few bits per second required for key redistribution. With newer smart card technology this can be increased to hundreds of kilobits per second. In this manner rebroadcasting will generally be effectively prevented.

Claims

1. System for decrypting an encrypted message, comprising first and second decryption devices, the first decryption device having a higher security than the second decryption device, means for dividing an encrypted message into blocks, and means for providing at least the first block of a message to the first decryption device and for providing a plurality of the further blocks of this message to the second decryption device, wherein an output of the first decryption device is used as input of the second decryption device, said second decryption device operating according to a block chaining method for decrypting said plurality of further blocks.

2. System according to claim 1, wherein said providing means provides each x^{th} block to the first decryption device.

3. System according to claim 1 or 2, wherein said second decryption device operates according to an error-propagating block chaining method.

4. System according to anyone of the preceding claims, wherein the first decryption device provides a clear text output.

5. System according to claim 1, 2 or 3, wherein the first decryption device provides a partially decrypted output, wherein the second decryption device first completes the decryption operation.

6. System according to anyone of the preceding claims, wherein the computing speed of said second decryption device is higher than the computing speed of the first decryption device.

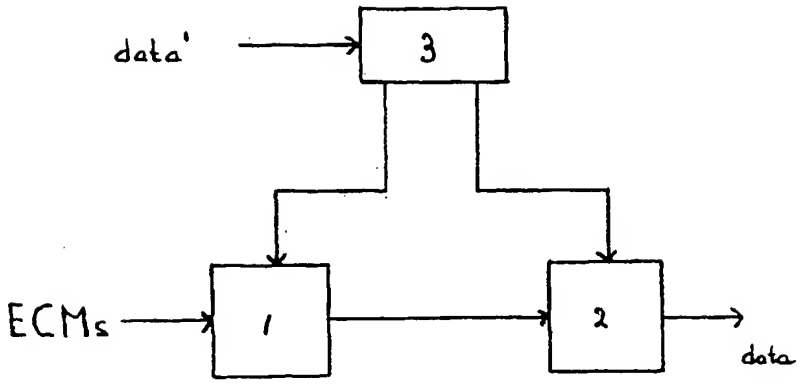
7. Method for distributing data in a system with a number of receivers, comprising the steps of dividing the data into blocks, encrypting at least the first block using a first key and encrypting a plurality of the further blocks according to a block chaining method using the first block as input vector, distributing the encrypted data to the receivers and distributing the first key in an encrypted message to the receivers.

8. Method according to claim 7, comprising the steps of receiving the encrypted data and the first key at a receiver, dividing the encrypted data into blocks, decrypting at least the first block in a first decryption device using the first key, decrypting a plurality of

further blocks in a second decryption device, the first decryption device having a higher security than the second decryption device, using an output of the first decryption device as input to the second decryption device and operating the second decryption device according to said block chaining method.

9. Method according to claim 7 or 8, wherein a second key is used in the block chaining method to encrypt said plurality of further blocks, wherein the first and second keys are distributed to the receivers in an encrypted message, the encrypted message being decrypted by the first decryption device, wherein the first decryption device forwards the second key and the first block to the second device.

10. Method according to claim 7, 8 or 9, wherein the first and each x^{th} block are encrypted using the first key or decrypted in the first decryption device using the first key, respectively.


data'
3
ECMs
1
2
data

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 20 2916

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 822 720 A (THOMSON MULTIMEDIA SA) 4 February 1998 * page 3, column 4, line 50 - page 7, column 11, line 47 * * figures 1-5 *	1,2,5, 7-10	H04N7/16 H04N7/167
X	EP 0 658 054 A (NEWS DATACOM LTD) 14 June 1995 * page 4, column 5, line 12 - page 6, column 9, line 38 * * figures 1-6 *	1,2,5, 7-10	
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, no. 266, 21 December 1995, pages 64-77, XP000559450 Grand Saconnex, CH * page 64, left-hand column, line 1 - page 67, left-hand column, line 2 * * page 64, right-hand column, line 25 - page 70, right-hand column, line 9 * * page 73, left-hand column, line 41 - page 74, right-hand column, line 7 *	1-8	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 January 1999	Van der Zaal, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 20 2916

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-01-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0822720 A	04-02-1998	FR 2751817 A	30-01-1998
		CN 1175142 A	04-03-1998
		JP 10098462 A	14-04-1998
EP 0658054 A	14-06-1995	IL 107967 A	05-12-1996
		AT 171331 T	15-10-1998
		AU 684112 B	04-12-1997
		AU 8034294 A	15-06-1995
		CA 2137608 A	10-06-1995
		DE 69413361 D	22-10-1998
		JP 7288522 A	31-10-1995
		US 5590200 A	31-12-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82